(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 718 999 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
26.06.1996 Bulletin 1996/26

(51) Int Cl.[6]: **H04L 1/00**, H03M 13/00, H03M 7/30, H04L 9/00

(21) Application number: **95203419.7**

(22) Date of filing: **08.12.1995**

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU NL PT SE

(30) Priority: **12.12.1994 NL 9402103**

(71) Applicant: **Koninklijke PTT Nederland N.V.**
NL-2509 CH The Hague (NL)

(72) Inventors:
- **Herrera van der Nood, José Manuel**
  NL-3028 XA Rotterdam (NL)
- **Trommel, Eric Simon**
  NL-2728 MP Zoetermeer (NL)

(54) Data transmission method and device simultaneously improving error protection and data integrity

(57) The invention relates to a method for transmitting data in a processed manner on a communication channel, in which a first series (1) of data is converted into a second series (2) of data by means of a first operation (P), the second series (2) of data is transmitted on the communication channel and the second series of data is then converted into a third series (3) of data by means of a second operation (P'). Check data (4) are formed on the basis of the first series (1) and are added to the second series (2). Subsequently, the integrity of the third series (3) is checked using the check data (4). The operations may comprise, respectively, data compression and data decompression. The check data are subjected to a protection operation (S) before they are added to the second series. Preferably, the method takes place at layer 3 of the so-called OSI model. The invention furthermore provides devices for using the method.

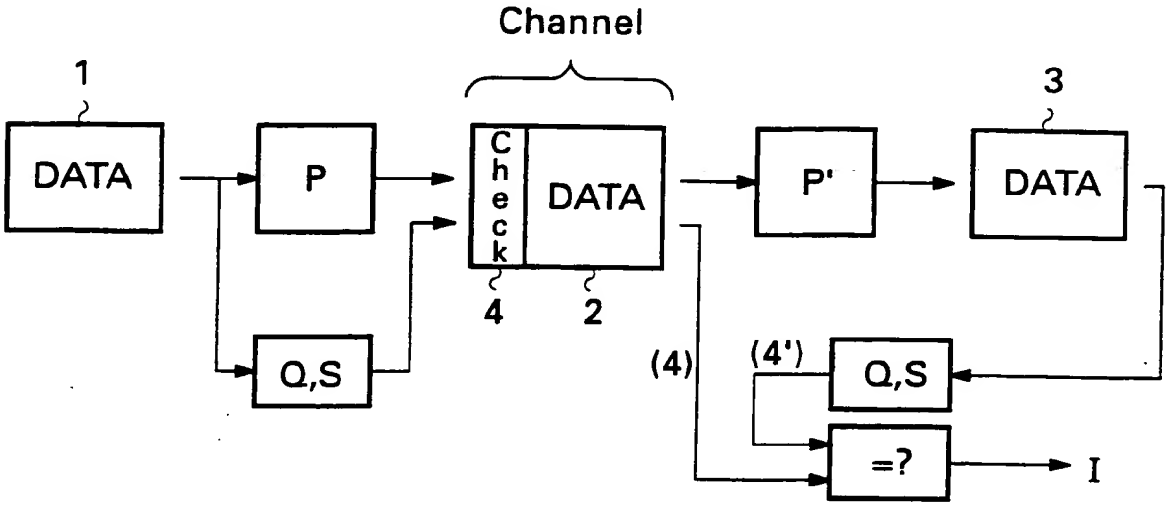

FIG. 1

EP 0 718 999 A2

Description

BACKGROUND OF THE INVENTION

The invention relates to a method and device for transmitting processed data on a communication channel. More particularly, the invention relates to a method for transmitting data in a processed manner on a communication channel, comprising the steps of: converting a first series of data into a second series of data by means of a first operation, generating check data on the basis of the first series, which check data are added to the second series, transmitting the second series of data on the communication channel, converting the second series of data into a third series of data by means of a second operation and checking the integrity of the third series using the check data.

It is known in practice to transmit data in a processed manner. In this connection, the problem arises that errors may occur during the transmission. The received data are corrupted by such transmission errors, as a result of which transmitted "zeros" are received as "ones" and vice versa. At the same time, the corruption is dependent on the operation concerned. In the case of data compression, in particular, errors make themselves felt to a considerable degree in the final (decompressed) data received, but also in the case of encryption, for example, only a few transmission errors may heavily corrupt the total message of the transmitted data.

This problem arises in particular in adaptive (de) compression of data, the tables on the basis of which the compression and decompression is carried out becoming permanently deranged by a transmission error. As a result, it is possible that the entire subsequent message is corrupted by a single transmission error.

Existing communication protocols often have a form of protection against transmission errors. Thus, for example, in the so-called OSI model, an error-correction protocol is laid down at layer 2 in order to be able to use data compression. Such a protocol does not, however, offer a complete protection against errors, such as bit errors, which occur in the transmission since the so-called checksum mechanism incorporated in existing protocols offers only a limited protection against errors.

SUMMARY OF THE INVENTION

The object of the invention is to eliminate the above-mentioned and other disadvantages of the prior art and to provide a method for transmitting data in a processed manner, which method offers greater protection against transmission errors in the case of compression or other data processing.

In addition the object of the invention is to provide a method for transmitting processed data, which method makes it possible to carry out an integrity verification on the data.

The object of the invention is furthermore to provide devices and a system for implementing the method.

For this purpose, a method of the type mentioned in the preamble is characterized, according to the invention, by the step of subjecting the check data to a protection operation before the check data are added to the second series.

By subjecting the check data to a protection operation, an indirect integrity check of the transmitted data is provided. The protection operation need not be performed upon the transmitted (compressed) data to be effective against changes in the transmitted data. Any changes in the transmitted (compressed) data, whether wilful or erroneous, will result in a discrepancy between the compressed data and the associated check data. The protection operation effectively inhibits an intentional modification of the check data. Thus, with the method of the present invention a high degree of protection against both transmission errors and deliberate data corruption is effectively obtained.

It should be noted that it is known per se to generate check data, such as parity bits, of data to be transmitted. Such parity bits are, however, always formed on the basis of the transmitted data itself, that is to say of the processed data (second series) if there is a processing operation prior to the transmission. However, the invention envisages using the unprocessed data (first series) for the formation of check data. This has, inter alia, the advantage that the so-called overhead, i.e. the added data, is well defined and can have a fixed length. This makes it possible to guarantee that the transmitted data fit into a certain window. In the case of, for example, data compression as processing operation, expansion of the check data due to unfavourable coding can be avoided in this way since the check data itself are not subjected to said operation. Furthermore, the invention envisages to subject the check data to a protection operation, preferably without performing such a protection operation upon the data proper.

If the processing comprises data compression, the formation of check data on the basis of the first (uncompressed) series offers the further advantage that the detection perception for check bits (such as parity bits) will be greater over a certain number of bytes in the first series than in the second series. In addition, a check bit itself contains in this way less information, as a result of which the occurrence of a transmission error in a check bit causes less information loss and will therefore have less disadvantageous consequences.

When, according to the invention a protection operation is carried out on the check data, a degree of data protection of the data transmission can be achieved. In the method according to the invention, the formation of check data may take place on the basis of various operations, that is to say not only the formation of parity bits but also, for example, the performance of a so-called hash function. The protection operation may, for example, comprise an enciphering operation or a parity

operation.

EXEMPLARY EMBODIMENTS

The invention will be explained in greater detail below by reference to the figures.

Figure 1 shows diagrammatically the transmission of data according to the invention.

Figure 2 shows diagrammatically a first device for implementing the invention to be used at the transmitting end of a communication channel.

Figure 3 shows diagrammatically a second device for implementing the invention to be used at the receiving end of a communication channel.

As is shown diagrammatically in Figure 1, at the transmitting end (left-hand side in Figure 1), a first series of data 1 is converted into a second series of data 2 by means of an operation P. The second series is transmitted on a communication channel, diagrammatically indicated by C, after which said second series 2 is converted into a third series 3 at the receiving end (right-hand side in Figure 1) by a further operation P', which is in most cases the inverse of operation P. If the operation P' is the inverse of P ($P' = P^{-1}$), the third series 3 will completely or at least partially correspond to the first series 1. If the operation P comprises a compression operation the operation P^{-1} is a decompression operation, and the third series 3 will correspond to series 1 if no transmission errors have occurred and no conversion of data format has been carried out.

According to the invention, check data 4 are formed in an operation Q using the first series 1. Said check data are added to the series 2 and transmitted. In this process, the check data 4 may be added to the series 2, for example, in a separate data block, but they may also be incorporated in the series 2 in a dispersed manner by means of interleaving. A combination of grouped and dispersed incorporation is also possible, for example in small groups of 4 bits, the small groups themselves being dispersed over the data of the series 2. As a result of dispersing the check data to a certain degree, a greater degree of protection is obtained against transmission errors occurring in groups, so-called bursts.

The check data may be formed by determining parity data in a known manner. In this case, one parity bit may be formed, for example, per byte of the first series. In general, a small group (for example 1, 2 or 3) of check bits (such as parity bits) will be formed on the basis of a number of bytes of the first series, and said number of bytes will be dependent on the properties of the data and of the communication channel C. Thus, in the case of a channel having a small number of errors (small bit error rate BER), one or a few check bits will suffice for a large number (for example, 10 or 20) of data bytes. It is also possible for the check bits to comprise, instead of parity bits, bits which have been formed by another operation Q, for example a so-called hash function.

At the receiving end, check data 4' are likewise formed from the series 3 by an operation Q. Said regenerated check data 4' are compared with the check data 4 incorporated in series 2. The integrity of the series 2 and 3 can be confirmed using this comparison.

Instead of the operation Q to which the third series 3 is subjected, an operation R to which the second series 2 is subjected can optionally be used at the receiving end. In this case, the operation R should have the property that it reconstructs the check data on the basis of the processed data (second series), or at least checks the integrity of the second series using the transmitted check data and the (processed) data of the second series.

In order to provide a form of protection for the series 2 which is transmitted on the communication channel C, the check data 4 may be subjected to a protection operation S. As a result, it is more difficult for unauthorized third parties to check the integrity of the data transmission (with the aid of the check data 4), with the result that third parties acquire no certainty about the presence of any errors in the data.

The protection operation S may comprise the enciphering of the check data, for example by the (modulo 2) addition of random numbers to the check data. In most cases, it will be necessary under these circumstances to incorporate a starting value in the second series in order to make it possible to decrypt (likewise by modulo 2 addition of the same random numbers) at the receiving end.

A simpler protection operation S comprises, for example, the alternating inversion, or inversion at certain intervals, of the check bits. Optionally, the protection operation S may comprise the addition to the check data of a value read out of a fixed table. Although a lesser degree of protection is thereby achieved, the transmission of a starting value can be avoided.

It will be clear that if an operation S is carried out at the transmitting end on the result of the operation Q, this will also have to take place at the receiving end.

The abovementioned operation P may also comprise an encryption or other coding operation. The operations P, P', Q, R and S may be operations known per se. Suitable operations may be found in e.g. R. N. Williams: "Adaptive Data Compression", Dordrecht, 1991, Chapter 1.16, and F. Rubin: "Cryptographic Aspects of Data Compression Codes", Cryptologia, Vol. 3, No. 4, October 1979.

The first, second and third series may be composed either of bit streams or of series of data packets, and the data packets may have an arbitrary length. Preferably, the first and third series are byte-oriented, and the second series is bit-oriented. Advantageously, the method according to the invention is carried out in such a way that the data are processed separately per channel or per subchannel. In this connection, the first series may contain data from different logic channels which are subjected to different operations (see also International Patent Application WO95/20285, which is herewith incor-

porated by reference in this text).

The method according to the invention is suitable, in particular, but not exclusively, for providing data compression at layer 3 (network layer) of the OSI model (as described in e.g. F. Mazda (Ed.): "Telecommunications Engineer's Reference Book", Oxford 1993, Chapter 12).

The device 10 shown in Figure 2 for implementing the method according to the invention comprises an input buffer 11, a processing unit 12, an output buffer 13 and a control unit 14. Data of the first series (1 in Figure 1) is buffered in the input buffer 11 and then processed in the processing unit 12 (for example compressed) under the control of the control unit 14. The data are then temporarily stored (if necessary) in the output buffer 13 as second series with the addition of check data, and it is then delivered to a communication channel (not shown).

The processing unit 12 comprises processing means, such as a microprocessor, and memory means, such as a random access memory (RAM) and/or a register for temporarily storing intermediate results (for example of a parity operation or a compression process). Suitable software (for example for the operation process) can be stored in a fixed, i.e. read only memory (ROM or EPROM). The control unit 14 which may likewise comprise a microprocessor and memory means (RAM/ROM) caters, inter alia, for the insertion (integration) of the check data into the processed data, for example by feeding said check data to suitable parts of the output buffer 13. The performance of an additional protection operation (S in Figure 1) may likewise be carried out by the processing means 12, but it may optionally also be carried out by separate additional processing means (not shown). Optionally, the output buffer 13 may be integrated into the processing unit 12.

If the series which are processed with the aid of the device 10 contain data of different (logic) channels or sub-channels, the output buffer may advantageously be provided with separate, channel-related buffer units, as described in International Patent Application WO95/20285.

Like the device 10 of Figure 2, the device 20 of Figure 3 comprises an input buffer 21, a processing unit 22, an output buffer 23 and a control unit 24, the structure of which may be identical to parts 11 - 14 of the device 10. The device 20 is furthermore provided with an extraction unit 25, an additional processing unit 26 and a comparison unit 27. The extraction unit 25, which may be integrated in the input buffer 21, extracts the check data from the received data (second series 2 in Figure 1). The additional processing unit 26, which may optionally be integrated in the processing unit 22, forms new check data on the basis of the received data and data reprocessed (in inverse form) in the processing unit 22. If a protection operation (S) is carried out at the transmitting end on the original check data, this should also be carried out on the new check data, for example by the additional processing unit 26, in order to make a meaningful comparison possible. The new check data are compared in the comparison unit 27 with the check data which were contained in the received series of data. If the (received) check data are identical to the new check data, this confirms the integrity of the received data and, consequently, the integrity of the series of data (third series 3 in Figure 1) which is delivered by the output buffer 23. If the (received) and new check data are not identical, an error has occurred in the data transmission. In that case a suitable signal can be delivered by the comparison unit 27. A retransmission of the data concerned, for example, may then be requested.

The devices 10 and 20 of Figures 2 and 3 can be produced in a manner known to the person skilled in the art from commercially available components. Advantageously, the devices 10 and 20 may be accommodated, separately or together, in one or more application-specific integrated circuits (ASICs).

As has been explained above, the invention provides, inter alia, a method for transmitting data in a processed manner (for example compressed) at layer 3 of the OSI model, an additional protection being offered against the occurrence of transmission errors. In addition, the protection may be used to provide a certain degree of data security without, however, having to subject the data itself to an additional (encryption) process.

It will be understood by those skilled in the art that the invention is not limited to the embodiments shown and that many modifications and additions are possible without departing from the scope of the invention.

Claims

1. Method for transmitting data in a processed manner on a communication channel, comprising the steps of:

   - converting a first series (1) of data into a second series (2) of data by means of a first operation (P),
   - generating check data (4) on the basis of the first series (1), which check data are added to the second series,
   - transmitting the second series (2) of data on the communication channel,
   - converting the second series (2) of data into a third series (3) of data by means of a second operation (P^{-1}), and
   - checking the integrity of the third series (3) using the check data (4),

   characterized by the step of

   - subjecting the check data (4) to a protection operation (S) before adding said check data (4) to the second series (2).

2. Method according to claim 1, wherein the checking of the integrity of the third series (3) of data comprises:

   - regenerating check data on the basis of the third series (3);
   - subjecting the regenerated check data (4') to the protection operation (S); and
   - comparing the result of this operation with the check data (4) of the second series (2).

3. Method according to claim 1, wherein the checking of the integrity of the third series (3) of data comprises:

   - regenerating check data on the basis of the third series (3);
   - subjecting the transmitted check data (4) to the inverse of the protection operation (S); and
   - comparing the result of this operation with the regenerated check data.

4. Method according to any of the preceding claims, wherein the protection operation (S) comprises an enciphering operation.

5. Method according to any of the preceding claims, wherein the protection operation (S) comprises a parity operation.

6. Method according to any of the preceding claims, wherein the check data (4) are interleaved with the data (2) of the second series.

7. Method according to any of the preceding claims, wherein the data (1) are associated with a plurality of subchannels, and wherein the data are separately processed per subchannel.

8. Method according to any of the preceding claims, wherein the processing comprises the compression of the data.

9. Method according to any of the preceding claims, wherein the transmission of data in a processed manner takes place at layer three of the OSI model.

10. Method according to any of the preceding claims, wherein the first (1) and third (3) series are constituted by data packets.

11. Device (10) for processing data, comprising means (11) for receiving data, means (12) for processing received data and means (13) for transmitting processed data, said means (12) for processing being arranged for the formation of check data on the basis of received data and for the addition of the check data to processed data, characterized in that the means (12) for processing are arranged for carrying out a protection operation on the check data.

12. Device according to claim 11, wherein the means (12) for processing comprise compression means.

13. Device according to claim 11 or 12, wherein the means (12) for processing are designed for interleaving the check data in the data to be transmitted.

14. Device (20) for processing data, comprising means (21) for receiving data, means (22) for processing received data and means (23) for transmitting processed data, means (25) for extracting first check data (4) from received data, means (26) for forming second check data (4') from processed data and means (27) for comparing the first and second check data, characterized in that the means (26) for forming second check data (4') are arranged for carrying out a protection operation (S) on the second check data.

15. Device according to claim 14, wherein the means (22) for processing data comprise decompression means.

16. Device according to one of claims 11 to 17 inclusive, provided with means for processing data per subchannel.

17. Device according to any of the claims 11 to 13 inclusive and/or 15 to 18 inclusive, accommodated in an application-specific integrated circuit.

18. Data communication system, designed for application of the method according to any of claims 1 to 10 inclusive.

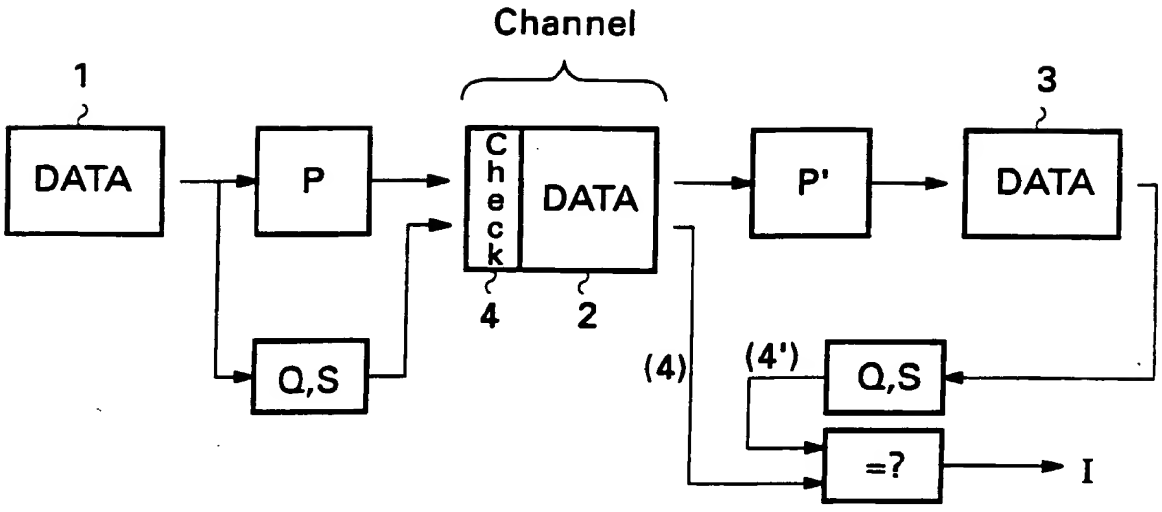

FIG. 1

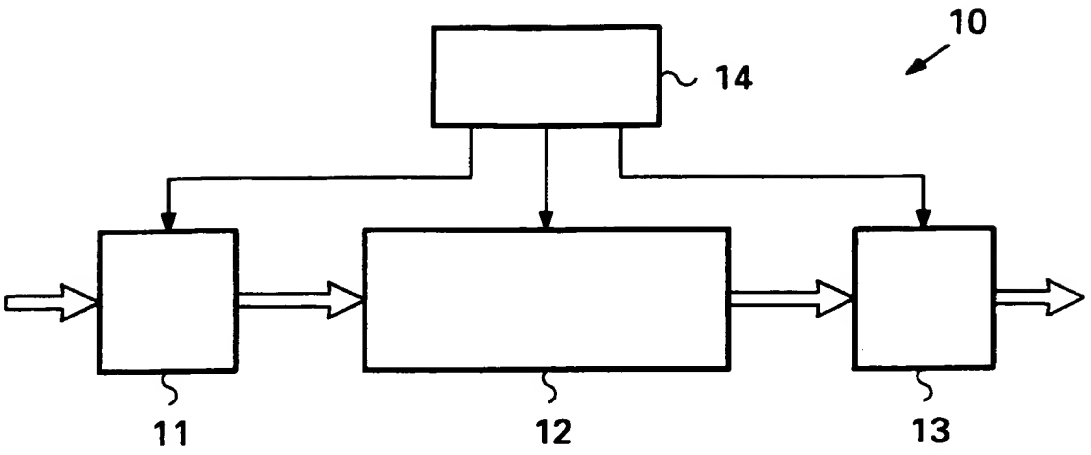

FIG. 2

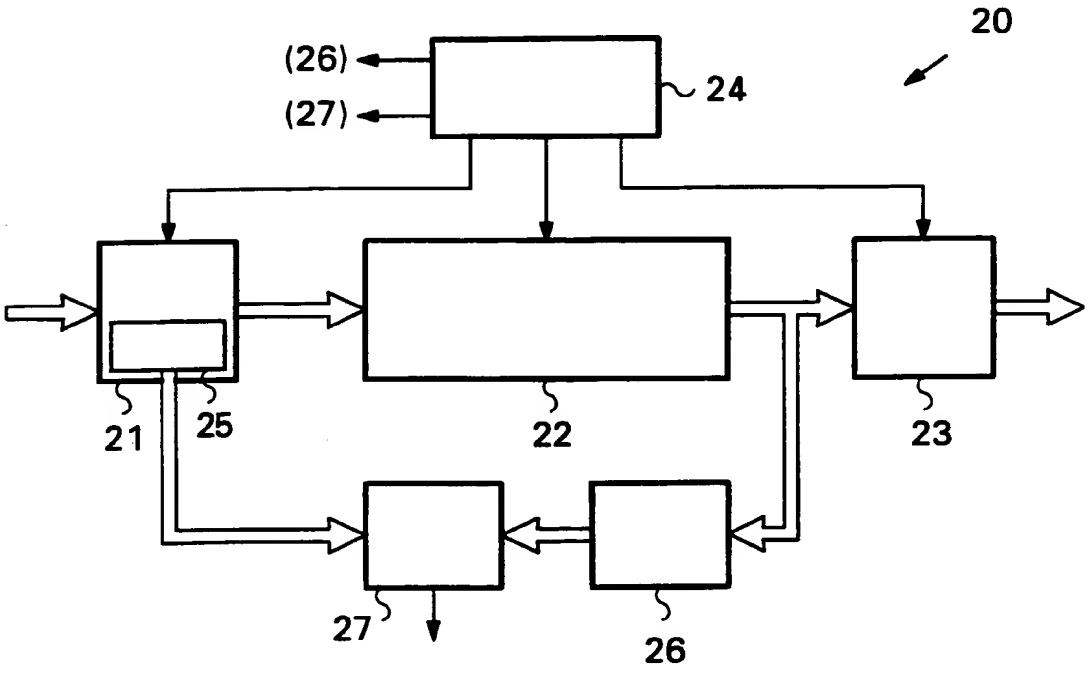

FIG. 3

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 718 999 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
01.10.1997 Bulletin 1997/40

(43) Date of publication A2:
26.06.1996 Bulletin 1996/26

(21) Application number: **95203419.7**

(22) Date of filing: **08.12.1995**

(51) Int Cl.[6]: **H04L 1/00**, H03M 13/00, H03M 7/30, H04L 9/00

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU NL PT SE

(30) Priority: **12.12.1994 NL 9402103**

(71) Applicant: **Koninklijke PTT Nederland N.V.**
2509 CH Den Haag (NL)

(72) Inventors:
- **Herrera van der Nood, José Manuel**
  NL-3028 XA Rotterdam (NL)
- **Trommel, Eric Simon**
  NL-2728 MP Zoetermeer (NL)

(54) Data transmission method and device simultaneously improving error protection and data integrity

(57) The invention relates to a method for transmitting data in a processed manner on a communication channel, in which a first series (1) of data is converted into a second series (2) of data by means of a first operation (P), the second series (2) of data is transmitted on the communication channel and the second series of data is then converted into a third series (3) of data by means of a second operation (P'). Check data (4) are formed on the basis of the first series (1) and are added to the second series (2). Subsequently, the integrity of the third series (3) is checked using the check data (4). The operations may comprise, respectively, data compression and data decompression. The check data are subjected to a protection operation (S) before they are added to the second series. Preferably, the method takes place at layer 3 of the so-called OSI model. The invention furthermore provides devices for using the method.

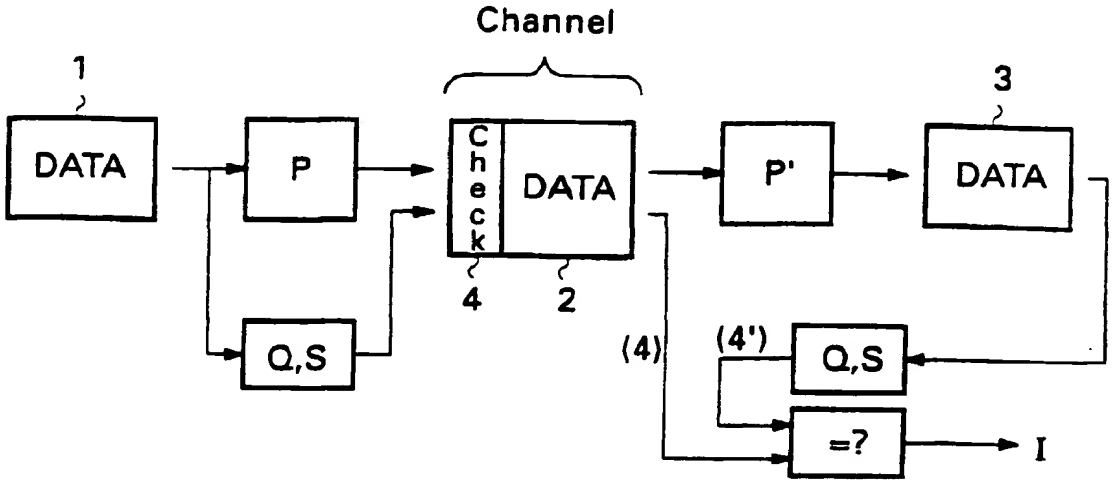

FIG. 1

EP 0 718 999 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 95 20 3419

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	WO 92 05647 A (NORTHERN TELECOM LIMITED) 2 April 1992 * page 2, line 10 - line 24 * * page 4, line 1 - line 11 * * page 5, line 11 - page 6, line 2 * * figures 1A,1B * ---	1-3,6, 10,11, 13,14,18	H04L1/00 H03M13/00 H03M7/30 H04L9/00
Y	US 4 929 946 A (O'BRIEN ET AL.)	1,2,4-8, 10-16,18	
A	* abstract; claims 1,2,10,11; figures 1,2,5 * * column 3, line 16 - line 21 * ---	9,17	
Y	US 4 654 480 A (WEISS)	1,2,4-8, 10-16,18	
A	* abstract * * column 4, line 61 - column 5, line 60 * * column 8, line 29 - line 57 * ---	9,17	
A	US 5 093 831 A (SERIZAWA ET AL.) * abstract; figure 2 * * column 1, line 23 - column 2, line 4 * ---	7,16	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L H03M G06F
A	WO 91 20076 A (STORAGE TECHNOLOGY CORPORATION) * page 30, line 20 - line 24; claims 1,3,12,14 * ---	8,12,15	
A	EP 0 564 825 A (NOKIA TECHNOLOGY GMBH) * column 1, line 40 - line 50 * * column 2, line 11 - line 39; claims 1-4; figure 1 * ---	4,18	
A	EP 0 191 410 A (HITACHI LTD.) * abstract * * page 4, line 19 - page 5, line 13 * * page 24, line 7 - line 11 * -----	6,13	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	31 July 1997	Ghigliotti, L

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filling more than ten claims

☐ All claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for all claims.

☐ Only part of the claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid,

namely claims:

☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirement of unity of invention and relates to several inventions or groups of inventions, namely:

See sheet -B-

☒ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid,

namely claims:

☐ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims,

namely claims:

European Patent Office

EP 95 20 3419 -B-

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirement of unity of invention and relates to several inventions or groups of inventions, namely:

1. Claims 1,2,4-18 : Data transmission method using error protection and checking the integrity of the received data by comparing the received check codes with the re-calculated check codes, calculated as a function of the decoded (i.e. decrypted or decompressed) data.

2. Claim 3 : Data transmission method using error protection and checking the integrity of the received data by comparing the received check codes with the inversely-calculated check codes, calculated as a function of the received encoded (i.e. encrypted or compressed) data.